Charte ministérielle d'utilisation des outils numériques

FÉVRIER 2018

SECRÉTARIAT GÉNÉRAL

Sommaire

Préambule

La présente charte a pour objet d'encadrer l'usage des outils numériques au sein des ministères économiques et financiers, en précisant :

- d'une part, les moyens mis en œuvre par l'administration, garante du respect de la législation et de la réglementation en vigueur et de la sécurité des systèmes d'information ;
- d'autre part, les règles que doivent respecter les utilisateurs des outils numériques mis à leur disposition.

Elle est applicable à toute personne physique, dénommée l'« utilisateur » [1] dans la suite du document, à qui l'usage d'un ou plusieurs outils numériques est consenti par l'administration.

L'usage des outils numériques par les représentants syndicaux fait l'objet de dispositions spécifiques.

Outre l'utilisation généralisée des outils numériques par les services des ministères économiques et financiers pour l'exercice de leurs missions, la profusion des outils mobiles (tablettes, smartphone, etc) et des usages de l'internet rendent par ailleurs la frontière entre vie professionnelle et vie privée de plus en plus perméable.

Les usages des ressources informatiques non conformes aux préconisations de la présente charte peuvent être regardés comme des fautes professionnelles susceptibles d'entraîner pour l'utilisateur une suspension conservatoire des outils mis à disposition, des sanctions disciplinaires, sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

Les prescriptions de cette charte peuvent être précisées ou complétées en tant que de besoin par des chartes directionnelles, des annexes techniques ou des dispositions spécifiques à certains services.

[1] Le terme utilisateur désigne toute personne physique quel que soit son statut (fonctionnaire, contractuel, salarié de société prestataire de service, stagiaire, vacataire, apprenti,...) et quel que soit son lieu d'exercice ou son mode de travail (sur site, en télétravail,...).

L’administration assure le respect de la réglementation en vigueur et met en œuvre une politique de sécurité des systèmes d’information et de communication

Le cadre juridique applicable

L’administration applique notamment les textes portant sur :

- la protection des données personnelles au titre de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que du règlement européen relatif « à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données » [UE 2016/679] 2 ;
- les droits et obligations des fonctionnaires, au titre des lois n° 83-634 du 13 juillet 1983 et n° 2016-483 du 20 avril 2016 ;
- l’obligation de collecte de traces sur internet au titre de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers ;
- le respect du droit d’auteur au titre de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI) ;
- la législation sur la propriété intellectuelle (code de la propriété intellectuelle) ;
- la lutte contre le téléchargement illégal au titre de la loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (dite loi HADOPI).
- L’accessibilité pour tous aux informations diffusées par les services de communication publique en ligne de l’Etat, des collectivités territoriales et des établissements publics qui en dépendent au titre de l’article 47 de la loi n°2005-102 du 11 février 2005 pour l’égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées (modifiée par l’article 106 de la loi n°2010-1321 du 7 octobre 2016 pour une République numérique) ;
- L’ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

- L'interopérabilité au sein des systèmes d'information de l'administration au titre de l'arrêté du 9 novembre 2009 (modifié par l'arrêté du 20 avril 2016) portant approbation du référentiel général d'interopérabilité (RGI) ;
- Les règles de sécurité au titre de l'arrêté du 6 mai 2010 (modifié par l'arrêté du 10 juin 2015) portant approbation du référentiel général de sécurité (RGS) ; l'administration assure le respect des objectifs et principes généraux de la politique générale de sécurité des systèmes pour l'administration (PGSSI des MEF du 1er août 2016[3]). Elle met notamment en place un processus de gestion des risques de sécurité des SI. Chaque entité administrative applique des procédures de surveillance afin de détecter les événements pouvant porter atteinte à la sécurité de ses SI et assure une gestion des incidents de sécurité ;
- Les conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature (décret n° 2016-151 du 11 février 2016, arrêté du 22 juillet 2016 pour les ministères économiques et financiers et arrêté du 26 janvier 2017 pour les directions départementales interministérielles) ;
- Les règles de protection appropriée des systèmes d'information sensibles contre toutes les menaces, qu'elles soient d'origine humaine ou non (Instruction interministérielle n°901 relative à la protection des systèmes d'information sensibles).

L'usage professionnel des outils numériques

Sauf consigne ou autorisation explicite les outils numériques mis à disposition par l'administration sont destinés à un usage professionnel.

Un usage privé est toléré à condition qu'il soit raisonnable, licite et qu'il n'affecte pas la sécurité et le fonctionnement normal des services.

Par défaut, les usages et contenus sont réputés professionnels ; seuls les espaces, répertoires, fichiers et/ou messages qualifiés expressément de « personnels » ou de « privés » seront considérés comme tels.

Dans tous les cas, y compris pour un usage privé, l'utilisation doit être conforme à l'ordre public et aux bonnes mœurs et ne doit pas mettre en cause ou porter atteinte à l'intégrité, à la réputation ou à l'image de l'administration (exemples : consultation de sites ou de contenus de nature pornographique, terroriste, de jeux, d'armes...).

L'usage privé des ressources informatiques peut être restreint par l'administration, notamment dans un souci de bon usage des ressources (sécurité, performance...).

En cas d'usage inapproprié au regard de la présente charte, l'agent peut voir suspendu ou retiré tout ou partie des moyens informatiques mis à sa disposition et peut voir restreints ses droits d'accès aux systèmes. Il pourra également faire l'objet d'une procédure disciplinaire.

[3] https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000033057599

Le contrôle des usages

L'administration met en œuvre des dispositifs de contrôle et de surveillance afin :

- de protéger les technologies et les informations de l'administration et des utilisateurs contre les actes illicites ou de malveillance ;
- d'assurer la sécurité des systèmes d'information ;
- de permettre leur emploi pour des usages professionnels dans des conditions optimales ;
- de s'assurer que les usages privés restent raisonnables ;
- de répondre aux exigences légales.

Ces mesures peuvent prendre la forme :

- de dispositifs de gestion des droits d'accès et des habilitations des utilisateurs des systèmes d'information et de communication ;
- de contrôles automatisés visant notamment la détection de virus ou logiciels malveillants, la prévention contre l'usurpation d'identité, la lutte contre les messages non sollicités, la prévention contre la fuite d'informations ou la suppression des comptes inutilisés. Les blocages qui pourraient en résulter sont explicités dans la mesure du possible par des messages d'information à l'utilisateur ;
- d'une surveillance, par le biais d'interceptions, des canaux de communication chiffrés, dans des cas spécifiques ;
- de dispositifs de collecte de données et de traces notamment pour :
    - les services de messagerie (messagerie électronique, sms, messagerie instantanée)[4] ;
    - l'accès à internet[5] ;
    - l'usage de la téléphonie[6] ;
    - l'usage des moyens d'impression et de reprographie ;
    - les actions réalisées par les utilisateurs dans certaines applications ou services[7].

Ces dispositifs sont mis en œuvre conformément au cadre légal et réglementaire en vigueur, et le cas échéant aux déclarations effectuées auprès de la Commission nationale de l'informatique et des libertés (CNIL), notamment la durée de conservation des traces.

[4]Ex : les identifiants, émetteur, nombre, volumétrie, fréquence d'envoi ou de réception, présence de pièces jointes (nature, volume, identification), classification, notamment entre privé et professionnel lorsque la mention est disponible.

[5]Ex : l'historique complet de navigation, volumétrie, durée, identifiant de l'utilisateur, adresse IP, protocoles utilisés.

[6]Ex : les identifiants (émetteur, destinataire), la volumétrie, la durée de communication.

[7]Ex : identifiants des équipements, utilisateurs, ressources et données, nature, date et volume des flux de connexion.

En cas de détection ou de présomption d'anomalies ou d'incidents de sécurité ou encore de présomption d'utilisation non conforme des outils mis à disposition, des actions de contrôle peuvent être exercées manuellement par les administrateurs et exploitants de la ressource informatique, notamment en vue de l'identification d'un fait fautif et de son auteur.

Ces données, même si elles relèvent de la tolérance d'usage privé, peuvent être communiquées aux autorités habilitées par la loi disposant d'un droit de communication sur ces données, notamment à l'autorité judiciaire qui en ferait la demande.

Les mesures particulières s'appliquant aux informaticiens

Le personnel informaticien met en œuvre et assure le bon fonctionnement des systèmes d'information, et notamment des dispositifs de sécurité de l'accès aux données.

Les exploitants et administrateurs qui assurent le fonctionnement des systèmes d'information mettent en œuvre des outils de supervision technique en conformité avec les règles de sécurité des systèmes d'information et celles relatives à la protection de la vie privée.

Seuls les personnels de la chaîne fonctionnelle sécurité des systèmes d'information (SSI) qui contribuent à la sécurité des systèmes informatiques peuvent mettre en œuvre des outils d'analyse, de surveillance et de contrôle de sécurité dans le cadre défini par leur hiérarchie, en conformité avec les règles de sécurité des systèmes d'information.

Les personnels informaticiens ne peuvent divulguer des informations professionnelles ou relatives à des utilisateurs, sauf dans le cadre de demandes d'autorités dûment habilitées (autorités judiciaires notamment).

Les services en charge des systèmes d'information signalent à leur hiérarchie tout usage abusif des ressources informatiques mises à disposition des utilisateurs : surcharge de la bande passante, téléchargements massifs, saturation des espaces disques partagés...

Un ensemble de droits et d'obligations s'applique aux utilisateurs des outils numériques

Les droits des utilisateurs

Ils bénéficient des mêmes droits que l'ensemble des citoyens, notamment :

- le respect de la vie privée tel qu'indiqué par l'article 9 du code civil ;
- la protection des données personnelles au titre de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que du règlement européen relatif « à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » [UE 2016/679] ;
- le secret des correspondances émises par la voie des communications électroniques, tel qu'indiqué dans l'article 226-15 du code pénal ;
- le respect de l'intimité de la vie privée (droit à l'image, paroles) tel qu'indiqué dans les articles 226-1 et 226-2 du code pénal ;
- le respect de la personne tel qu'indiqué par l'article 16 du code civil ;
- la liberté syndicale telle que visée par la décision n° 89-257 DC du 25 juillet 1989 ;
- la protection des mineurs au titre de la loi n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance ;
- la protection contre le harcèlement et la discrimination, en particulier le chapitre quatre du titre II de la loi n° 2002-73 du 17 janvier 2002 de modernisation sociale, la loi n° 2012-954 du 6 août 2012 relative au harcèlement sexuel et loi n° 2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de la lutte contre les discriminations ;
- le droit à la déconnexion tel qu'introduit par la loi du 8 août 2016 ;
- le droit à la portabilité des données relatives à la personne concernée tel qu'introduit par l'article 20 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, offrant aux personnes la possibilité d'avoir communication de leurs données personnelles détenues par l'administration dans un format ouvert et lisible ;
- l'article 47 de la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées, fait de l'accessibilité une exigence pour tous les services de communication publique en ligne de l'État, des collectivités territoriales et des établissements publics qui en dépendent. Il prévoit que les informations diffusées par ces services doivent être accessibles à tous ;
- l'accès libre à l'information syndicale de leur choix, pour les utilisateurs relevant de l'administration.

Les devoirs des utilisateurs

Les utilisateurs respectent les obligations générales de réserve, de probité, de neutralité, de respect du secret et de discrétion professionnels. Ils veillent notamment à :

- ne pas tenir des propos contraires à l'ordre public, diffamatoires, racistes, xénophobes, homophobes, portant atteinte à la décence, constituant une diffusion de fausse nouvelle... ;
- ne pas faire un usage des ressources informatiques qui puisse mettre en doute la neutralité du service public (respect du principe de laïcité, du devoir de réserve au regard notamment de leurs opinions politiques...) ;
- ne pas abuser de leurs fonctions en utilisant à des fins personnelles les applications informatiques professionnelles ;
- ne pas divulguer à des personnes non autorisées, ou n'ayant pas le besoin d'en connaître, des informations confidentielles détenues dans le cadre professionnel ;
- protéger l'accès des données professionnelles par un tiers non autorisé quel que soit le support de stockage de ces données (clés USB, terminaux, disques durs externes,...) ;
- ne communiquer en aucun cas leurs identifiants, mots de passe et/ou clés d'authentification à qui que ce soit, y compris à l'assistance informatique et à signaler immédiatement la perte ou la compromission d'une clé d'authentification, de supports contenant des données ou de tout autre matériel informatique appartenant à l'administration ;
- changer régulièrement leurs mots de passe ;
- ne pas télécharger de pièces jointes de messages électroniques dont le contenu ou l'origine paraissent douteux, et ne pas cliquer sur des liens qui leur paraîtraient suspects.
- ne pas empêcher ou différer au-delà d'une journée la mise à jour des systèmes d'exploitation et des logiciels, notamment de sécurité sur leur poste de travail.

Ils utilisent les ressources informatiques mises à leur disposition de façon responsable et économe :

- Ils font un usage raisonné de la messagerie électronique en veillant notamment à bien cibler les destinataires et à éviter les envois inutiles, notamment avec des pièces jointes volumineuses ;
- ils limitent les impressions sur papier à ce qui est nécessaire ;
- ils éteignent l'alimentation électrique de leur poste de travail en cas d'absence prolongée sauf consigne ponctuelle provenant de l'assistance informatique.

Les utilisateurs respectent les mesures de sécurité informatique mises en place par l'administration et participent aux actions de sensibilisation à la sécurité des systèmes d'information et de communication proposées par l'administration.

En cas de perte ou de vol d'un matériel mis à disposition par l'administration, de dysfonctionnements, comportements anormaux ou d'incidents sur les ressources informatiques, les utilisateurs sont tenus de les signaler à leur responsable hiérarchique et à leur service d'assistance informatique.

Cas particulier du maniement des données sensibles :

Dans certains services comportant des données sensibles, l'administration édicte des règles auxquelles les utilisateurs sont tenus de se conformer. Les informations classifiées, en particulier, font l'objet de dispositions spécifiques.

Lorsqu'ils traitent d'informations qualifiées de « sensibles » par l'administration ou par ses interlocuteurs (partenaires, fournisseurs, usagers...), les utilisateurs doivent avoir recours aux moyens de chiffrement mis à leur disposition par ceux-ci afin de les protéger d'un risque de compromission.

Principaux cas d'application de cette charte

Postes de travail et terminaux mobiles

L'administration fournit aux utilisateurs le matériel informatique et de téléphonie nécessaire à l'exercice de leurs fonctions (ordinateur fixe ou portable, éventuellement : tablette, smartphone, clefs USB, disques externes,...).

Les utilisateurs doivent *a minima* respecter les règles suivantes :

- ne pas modifier les paramétrages techniques et les politiques de sécurité et ne pas empêcher les mises à jour des matériels et/ou logiciels informatiques qui leur sont remis ;
- ne pas installer de logiciels non autorisés par le service informatique ;
- ne pas détourner l'usage des ressources informatiques qui leur sont allouées ;
- utiliser les ressources informatiques en tant qu'outils principalement liés à leurs activités professionnelles et non à leurs activités privées ;
- ne pas afficher leur mot de passe sur un support papier ou numérique et ne pas le partager avec d'autres personnes, ce qui n'exclut pas l'usage de coffre-fort électronique (cf § 3.3) ;
- déconnecter leur matériel ou verrouiller leur session lorsqu'ils s'absentent, même temporairement ;
- ne pas empêcher l'accès à leur poste de travail professionnel aux utilisateurs chargés de la maintenance des matériels, que ce soit de façon physique (ex : débrancher volontairement les câbles d'alimentation) ou informatique ;
- ne pas empêcher l'accès des personnes habilitées aux données professionnelles auxquelles elles peuvent avoir accès ;
- déclarer sans délai tout vol ou perte d'un matériel à leur supérieur hiérarchique, aux services de police et à l'assistance informatique ;
- ne pas laisser leur poste de travail sans surveillance, en particulier en dehors des locaux de l'administration lorsqu'il est portable ;
- stocker leurs données sur des supports sauvegardés : serveurs bureautiques, solution de gestion électronique des documents (GED) ;
- s'assurer que les données stockées localement sur le poste de travail sont sauvegardées (si ce n'est pas le cas, l'administration peut fournir aux utilisateurs un support afin que ceux-ci sauvegardent régulièrement les données hébergées localement sur le poste. Le support ne doit pas quitter les locaux de l'administration) ;
- le stockage de fichiers personnels est toléré à condition d'être limité dans le volume et dans la durée de conservation ;
- ne pas utiliser de matériel personnel à des fins professionnelles, sauf s'il s'agit d'utiliser des outils mis à disposition par l'administration à cette fin (ex : consultation de la messagerie professionnelle depuis internet...) ;

- ne pas connecter au réseau professionnel ou utiliser des équipements qui ne sont pas fournis ou n'ayant pas fait l'objet d'un contrôle par l'administration (clefs USB,...) ;
- en cas de prise en main de son poste de travail par l'assistance informatique (PMAD) :
    - être vigilant et notamment rester présent devant son poste de travail durant l'intervention ;
    - fermer les applications informatiques et les fichiers ouverts sur son poste de travail, notamment les documents sensibles ou classifiés ;
    - mettre fin à la PMAD s'il estime qu'il existe un risque de sécurité ;
    - s'assurer que la session de PMAD est fermée en fin d'intervention.

Cas particulier des ordinateurs portables et des tablettes

Ces matériels sont destinés à un usage professionnel.

Ils ne doivent pas être prêtés à des tiers.

En dehors des connexions directes au réseau professionnel, les accès aux réseaux en mobilité (wifi ou autres) ne sont autorisés que *via* des logiciels fournis par l'administration, par exemple par l'emploi d'un VPN (virtual private network).
La connexion directe à Internet est interdite.

La messagerie électronique

Dans le respect de la charte de bon usage de la messagerie, les utilisateurs doivent respecter les règles d'usage suivantes :

- faire un usage raisonné de la messagerie et ne pas surcharger les boîtes de messagerie internes ou externes ;
- ne pas diffuser de messages de type canulars (hoax), chaînes, escroquerie par hameçonnage (phishing), jeux, paris,... ;
- ne pas utiliser leur adresse électronique professionnelle dans un contexte non professionnel, en particulier, ne pas l'utiliser sur des sites internet (groupes de discussion (chats), commerce, forums, blogs, etc...), sans rapport avec l'activité professionnelle ;
- ne pas rediriger manuellement ou automatiquement les messages professionnels qu'ils reçoivent sur leur messagerie professionnelle vers une messagerie personnelle ;
- ne pas utiliser leurs adresses de messageries personnelles dans un contexte professionnel ;
- s'assurer, à chaque envoi de données, en particulier sensibles, que la liste de diffusion ne comporte pas de destinataire inapproprié ;
- ne pas ouvrir les messages douteux et les pièces jointes suspectes, ne pas répondre aux émetteurs, et ne pas cliquer sur les liens présents dans ces messages (même s'ils se présentent comme des liens de « désabonnement ») ;
- prévenir l'assistance informatique en cas de doute ou après avoir ouvert un message ou cliqué sur un lien qui s'avère *a posteriori* douteux.

Tout message électronique envoyé depuis la messagerie professionnelle engage non seulement la responsabilité et l'image de l'utilisateur mais aussi celle de l'administration.

Afin de ne pas induire en erreur les destinataires, seuls les agents titulaires ou les contractuels disposant d'un contrat de travail avec l'administration peuvent disposer d'une adresse personnelle de l'organisation. Si le besoin est avéré, une adresse de messagerie peut toutefois être fournie à des personnes extérieures ou à des prestataires, dès lors que le libellé de l'adresse mél fournie par l'administration permet de les identifier comme tels.

Les identifiants et mots de passe

La plupart des services, qu'ils soient professionnels ou publics, requièrent une authentification.

Les utilisateurs doivent respecter les règles suivantes :

- les moyens d'authentification (identifiant/mot de passe, certificat/code pin, adresse de messagerie ou autres) fournis par l'administration sont strictement personnels, confidentiels et incessibles ;
- les mots de passe choisis doivent être suffisamment robustes (combinaison de lettres en minuscules, majuscules, chiffres, caractères spéciaux, absents du dictionnaire et sans lien évident avec l'utilisateur) ;
- ils doivent être modifiés régulièrement ;
- les moyens d'authentification professionnels doivent être utilisés pour des usages uniquement professionnels ;
- les mots de passe à usage privé ne doivent pas être utilisés dans le cadre professionnel et réciproquement ;
- la signature de documents par un certificat numérique émis par l'administration est réservée à un usage professionnel.

Les services informatiques peuvent mettre à la disposition des utilisateurs un « coffre-fort logiciel » de gestion des mots de passe pour aider à leur mémorisation. Ce dictionnaire doit rester strictement professionnel.

Habilitation des utilisateurs

Les utilisateurs accèdent aux ressources informatiques (réseaux, applications, serveurs...) dans la limite des droits d'accès qui leur sont accordés par le biais de mécanismes d'habilitation.

En application du principe du « moindre privilège », l'utilisateur ne doit disposer sur les ressources informatiques que des privilèges nécessaires à la conduite des actions relevant de sa mission.

Les privilèges permettant l'administration technique de ces ressources doivent être strictement réservés aux équipes en charge de l'exploitation et du support, et utilisés uniquement pour les actions d'administration le nécessitant.

La dérogation à ces règles doit faire l'objet d'une justification formelle par le responsable hiérarchique de l'utilisateur, et cela en concertation avec le responsable de la politique de sécurité de l'entité. L'utilisateur doit être sensibilisé aux responsabilités et risques de compromission des ressources informatiques associés à l'utilisation ces privilèges spécifiques.

L'accès à internet

Sauf contrainte particulière, l'accès des agents à internet est autorisé, notamment pour leur permettre d'assurer au mieux leur mission.

Afin d'assurer le respect des obligations qui lui incombent dans ce cadre, l'administration met en place :

- des dispositifs de filtrage des accès à internet, qui limitent l'accès aux seules catégories de sites autorisées ;
- des mécanismes de collecte des informations de connexion des utilisateurs à internet.

Les besoins métiers de certains utilisateurs pourront justifier la levée totale ou partielle des restrictions d'accès à internet (services d'enquêtes, de lutte contre la fraude sous réserve de la validation du responsable de la sécurité des systèmes d'information). L'adaptation des règles de filtrage est mise en œuvre par les services informatiques.

De manière générale, les utilisateurs sont invités à faire preuve de sens critique vis-à-vis des contenus disponibles sur internet hors sources réglementaires fiables (législation européenne, nationale, information institutionnelle).

Il est également rappelé que certains sites internet sont régis par le droit d'autres États n'offrant pas de garanties de protection des données personnelles. Les utilisateurs sont incités à prendre toutes les précautions utiles lorsqu'ils les consultent.

Le télétravail

Le télétravail désigne une forme d'organisation du travail dans laquelle un travail, qui aurait pu être exécuté dans les locaux de l'administration, est effectué par un agent hors de ces locaux, de façon régulière et volontaire en utilisant les technologies de l'information et de la communication. Il se pratique au domicile de l'agent – entendu comme le lieu de sa résidence habituelle – ou, le cas échéant, dans des locaux professionnels distincts de son lieu d'affectation.

Conformément à l'arrêté du 22 juillet 2016 portant application, dans les ministères économiques et financiers, de l'article 7 du décret n°2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature, le télétravailleur bénéficie des mêmes droits et est soumis aux mêmes obligations que les agents travaillant sur site, tels que décrits dans la présente charte.

L'administration met à la disposition de l'agent le matériel lui permettant d'exercer son activité professionnelle à son domicile et en assure la maintenance. Les équipements fournis restent la propriété de l'administration.

Le télétravailleur ne peut utiliser un autre matériel que celui fourni par l'administration. Il s'engage à réserver l'usage des équipements mis à disposition par l'administration à un usage strictement professionnel et à prendre soin de l'équipement qui lui est confié.

Les règles relatives à la sécurité des systèmes d'information et de protection des données pour les agents en fonctions sur site s'appliquent aux agents en télétravail. Ainsi, ceux-ci doivent se conformer aux règles relatives à la sécurité des systèmes d'information et veiller à l'intégrité et à la bonne conservation des données auxquelles ils ont accès dans le cadre professionnel.

Les télétravailleurs ne doivent pas installer de logiciels non autorisés par le service informatique sur le matériel qui leur a été fourni et doivent veiller à réaliser régulièrement une sauvegarde des travaux qu'ils effectuent sur un support externe.

Ils s'engagent également à respecter la confidentialité des informations détenues ou recueillies dans le cadre de leur activité et à veiller à ce qu'elles ne soient pas accessibles à des tiers.

Ils informent sans délai leur responsable hiérarchique ainsi que le service d'assistance informatique en cas de panne, de mauvais fonctionnement, de détérioration, de perte ou de vol du matériel mis à disposition.

Les services accessibles depuis un poste de travail non professionnel

L'administration peut mettre à disposition des utilisateurs des services en accès public depuis un poste de travail non professionnel (accès externe à la messagerie ou à des applications professionnelles,...) ou depuis un poste de travail professionnel.

Dans ce cas, elle peut mettre en place des contrôles visant à assurer la traçabilité de l'appareil utilisé pour la connexion et la sécurité du système d'information (antivirus présent, logiciels mis à jour régulièrement,...).

S'il s'est connecté au service depuis un poste de travail non professionnel, l'utilisateur supprime en fin de session les données issues du service consulté (ex : historique des cookies et fichiers professionnels téléchargés depuis le service). Une vigilance tout particulière s'impose lorsque l'utilisateur accède au service depuis un poste de travail public.

Les déplacements à l'étranger ou chez des tiers

Lors des déplacements à l'étranger ou chez des tiers, une vigilance particulière s'impose. Les utilisateurs doivent notamment respecter les règles suivantes :

- éviter de partir avec des données sensibles ;
- privilégier l'accès aux données sensibles via des connexions sécurisées plutôt qu'un stockage sur les équipements nomades (ordinateur portable, smartphone,...) ;
- sauvegarder les données et conserver la sauvegarde en lieu sûr ;
- ne pas utiliser des matériels qui ne sont pas fournis par l'administration (clefs USB, ordinateurs publics,...) ;
- ne pas se séparer de son matériel.

Les réseaux sociaux « grand public »

Les réseaux sociaux « grand public»[8] permettent des échanges d'intérêt général ou ciblés, purement privés ou ayant des liens potentiels avec l'activité professionnelle de l'agent. Accessibles depuis les équipements personnels de l'agent (PC, tablette, smartphone...) et éventuellement depuis les équipements professionnels (dans la limite des autorisations d'accès), ils sont hébergés chez des tiers, et bénéficient d'une audience large, souvent mondiale.

Les agents peuvent utiliser ces réseaux sociaux en restant soumis aux mêmes droits et obligations que dans le « monde réel ». Ils sont responsables des contenus (image, vidéo, texte...) et commentaires qu'ils publient, et doivent en assumer les conséquences, y compris sur le plan professionnel, dans un contexte où :

- la frontière entre le cadre professionnel et la vie privée est perméable sur les réseaux sociaux ;
- il est possible d'identifier qui utilise un pseudonyme ou un « avatar », et de recouper les informations présentes sur différents réseaux sociaux (ex : contenus « professionnels » sur Linkedin, contenus « privés » sur Facebook, hobbies sur des sites thématiques...) ;
- les réseaux sociaux jouent un rôle d'amplificateur, où les contenus peuvent être repris ou relayés par des tiers.

Ainsi, même s'il utilise un « avatar » ou un pseudonyme, l'utilisateur doit veiller à :

- ne pas utiliser son adresse de messagerie professionnelle, mais toujours utiliser une adresse de messagerie personnelle (Gmail, Yahoo...) ;
- privilégier l'utilisation d'un mot de passe complexe ;
- configurer les paramètres de confidentialité de son profil pour limiter les risques d'intrusion sur les plateformes de réseaux sociaux ou d'usurpation de son identité, penser à les vérifier régulièrement et bien réfléchir avant d'activer l'option de géolocalisation ;
- s'exprimer avec prudence, retenue et courtoisie et de se comporter comme dans n'importe quel lieu social, avec les mêmes règles de savoir-vivre ; s'abstenir de tous propos et commentaires abusifs, injurieux, diffamatoires ou incitant à la haine ou à la discrimination ;
- publier des images, photos libres de droit ou dont il est propriétaire ;

[8] Exemples : Facebook, Twitter, Snapchat, Linkedin, Viadeo, Google+, Instagram...

- ne pas publier de contenus et ne pas citer de personnes sans disposer de leur accord préalable (respect de la vie privée, droit à l'image) et des droits adéquats (droits d'auteur, droit des marques...) ;
- ne pas divulguer d'informations précises qui pourraient être utilisées à son encontre, pour nuire à des tiers (famille, collègues...) ou pour porter atteinte bon fonctionnement du service (vérifier par exemple les arrière-plans des photos et vidéos mis en ligne, qui peuvent permettre d'identifier un lieu, un équipement, une personne...) ;
- ne pas publier ou relayer de faux commentaires (faux avis, faux témoignages, dans le cadre de retweet par exemple...) et choisir avec soin avec qui partager un contenu ;
- ne pas mettre en ligne, sauf autorisation expresse, de document professionnel (textes, photos, vidéos, audio), étant précisé que le relais et/ou le partage d'informations publiées officiellement par les ministères économiques et financiers ne soulève pas de difficultés et peut être encouragé ;
- ne pas se prévaloir de sa qualité d'agent public ou mettre en avant ses fonctions pour appuyer ses publications ou contributions.

Par exception, certains agents peuvent être mandatés par leur hiérarchie pour s'exprimer sur certains réseaux sociaux au nom des ministères économiques et financiers ou de leur service (services communication, experts...). Par défaut, les règles ci-dessus s'appliquent, sauf si une consigne différente est donnée en considération de la mission confiée à l'agent (utilisation de la messagerie ou d'outils professionnels, contenus ou informations pouvant être publiés...).

Les services de téléchargement et de *streaming*

Le téléchargement de fichiers et l'accès aux ressources en *streaming* doit s'effectuer dans le respect de la réglementation en vigueur.

L'administration peut limiter ou interdire le téléchargement de certains fichiers volumineux ou présentant un risque pour la sécurité des systèmes d'information et de communication (virus susceptibles d'altérer le bon fonctionnement du système d'information, codes malveillants, programmes espions,...) ou l'accès à certaines ressources en *streaming*.

Même si l'accès aux sites est possible, l'utilisateur doit faire preuve de vigilance lorsqu'il télécharge un fichier provenant d'une source non professionnelle.

Les services de stockage et de partage sur Internet

L'utilisation de services sur internet non mis à disposition par l'administration tels que des outils de stockage (par exemple et de manière non exhaustive OneDrive ou Google Drive), de rédaction communautaire ou d'assistance à distance (prise en mains à distance) ou de visioconférence est interdite. L'utilisation de solution de visioconférence en tant que participant est tolérée dès lors qu'il n'y a pas de logiciel spécifique sur le poste de travail.

Même si l'accès aux sites est possible, l'utilisateur doit faire preuve de vigilance lorsqu'il télécharge un fichier provenant d'une source non professionnelle.

Par exception, les projets collaboratifs conduits avec certains acteurs (tiers de confiance, entreprises partenaires...) pourront justifier la levée totale ou partielle des restrictions d'accès à ces outils de stockage ou de partage, sous réserve de la validation du responsable de la sécurité des systèmes d'information.

La téléphonie

La téléphonie fixe professionnelle est mise à disposition des utilisateurs pour l'exercice de leur activité professionnelle.

L'administration peut limiter l'accès à certaines fonctions qui ne sont pas nécessaires aux activités professionnelles de l'utilisateur (appels internationaux, numéros surtaxés, etc...).

De plus, il est interdit de transférer la ligne fixe vers un numéro externe à l'administration sauf en cas d'autorisation explicite et écrite des autorités compétentes, par exemple dans le cadre du télétravail.

Application de la charte

La présente charte s'applique immédiatement à tout utilisateur visé en préambule et pourra faire l'objet de révisions, en fonction des évolutions technologiques et juridiques du Système d'Information et de ses impératifs de sécurité.

bercynumérique

www.bercynumerique.finances.gouv.fr

LABEL DIVERSITÉ
AFNOR CERTIFICATION
www.afnor.org

SG
Direction des Ressources humaines
Secrétariat général